OCHRONA DANYCH OSOBOWYCH W ADMINISTRACJI PUBLICZNEJ

Paweł Fajgielski

MONOGRAFIE

Wolters Kluwer

OCHRONA DANYCH OSOBOWYCH W ADMINISTRACJI PUBLICZNEJ

Paweł Fajgielski

MONOGRAFIE

Wolters Kluwer

WARSZAWA 2021

SERIA **MONOGRAFIE**

Stan prawny na 30 czerwca 2021 r.

Paweł Fajgielski, nr ORCID: 0000-0002-4293-1917

Recenzent
Dr hab. Arwid Mednis (WPiA UW)

Wydawca
Monika Pawłowska

Redaktor prowadzący
Joanna Tchorek

Opracowanie redakcyjne
Agnieszka Witczak

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

ISBN 978-83-8246-291-3 *ISBN PDF-a: 978-83-8246-605-8*
ISSN 1897-4392

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

Akty prawne

dyrektywa 95/46	–	dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. WE L 281, s. 31) – nieobowiązująca
dyrektywa 2016/680	–	dyrektywa 2016/680 Parlamentu Europejskiego i Rady (UE) z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89)
k.c.	–	ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2020 r. poz. 1740 ze zm.)
k.k.	–	ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2020 r. poz. 1444 ze zm.)
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)
konwencja 108	–	Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2003 r. Nr 3, poz. 25)
k.p.	–	ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2020 r. poz. 1320 ze zm.)
k.p.a.	–	ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2021 r. poz. 735)

rozporządzenie 2016/679	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1)
rozporządzenie KRI	–	rozporządzenie Rady Ministrów z 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247)
u.d.i.p.	–	ustawa z 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 r. poz. 2176)
u.e.l.	–	ustawa z 24.09.2010 r. o ewidencji ludności (Dz.U. z 2021 r. poz. 510 ze zm.)
u.i.d.p.	–	ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 670 ze zm.)
u.o.d.o.1997	–	ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.) – akt archiwalny
u.o.d.o.2018	–	ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 ze zm.)
u.p.e.a.	–	ustawa z 17.06.1966 r. o postępowaniu egzekucyjnym w administracji (Dz.U. z 2020 r. poz. 1427 ze zm.)
u.s.g.	–	ustawa z 8.03.1990 r. o samorządzie gminnym (Dz.U. z 2020 r. poz. 713 ze zm.)
u.s.p.	–	ustawa z 5.06.1998 r. o samorządzie powiatowym (Dz.U. z 2020 r. poz. 920 ze zm.)
u.s.w.	–	ustawa o 5.06.1998 r. o samorządzie województwa (Dz.U. z 2020 r. poz. 1668 ze zm.)

Czasopisma, publikatory i zbiory orzecznictwa

Dz.U.	–	Dziennik Ustaw
Dz.Urz. UE/WE	–	Dziennik Urzędowy Unii Europejskiej/Wspólnot Europejskich
MoP	–	Monitor Prawniczy

M.P.	–	Dziennik Urzędowy Rzeczypospolitej Polskiej „Monitor Polski”
ONSAiWSA	–	Orzecznictwo Naczelnego Sądu Administracyjnego i Wojewódzkich Sądów Administracyjnych
OSNC	–	Orzecznictwo Sądu Najwyższego. Izba Cywilna
OTK-A	–	Orzecznictwo Trybunału Konstytucyjnego, Seria A
PiP	–	Państwo i Prawo

Inne

ABI	–	administrator bezpieczeństwa informacji
BIP	–	Biuletyn Informacji Publicznej
CBOSA	–	Centralna Baza Orzeczeń Sądów Administracyjnych
CEIDG	–	Centralna Ewidencja i Informacja o Działalności Gospodarczej
CUW	–	centrum usług wspólnych
ePUAP	–	Elektroniczna Platforma Usług Administracji Publicznej
GIODO	–	Generalny Inspektor Ochrony Danych Osobowych
GOPS	–	Gminny Ośrodek Pomocy Społecznej
IOD	–	inspektor ochrony danych
NSA	–	Naczelny Sąd Administracyjny
OECD	–	Organizacja Współpracy Gospodarczej i Rozwoju
PESEL	–	Powszechny Elektroniczny System Ewidencji Ludności
RDK	–	Rejestr Danych Kontaktowych
SN	–	Sąd Najwyższy
TSUE	–	Trybunał Sprawiedliwości Unii Europejskiej
TK	–	Trybunał Konstytucyjny
UODO	–	Urząd Ochrony Danych Osobowych
USC	–	Urząd Stanu Cywilnego
WSA	–	Wojewódzki Sąd Administracyjny

WSTĘP

Realizacja większości zadań administracji publicznej wymaga przetwarzania danych osobowych. Organy administracji gromadzą, wykorzystują i udostępniają bardzo wiele informacji dotyczących osób fizycznych. Przez wiele lat informacje te były gromadzone w przeważającej większości na nośnikach papierowych (m.in. w aktach postępowania oraz w różnorodnych kartotekach i ewidencjach) i były przetwarzane w sposób tradycyjny (ręcznie), co sprawiało, że ilość danych była ograniczona, dostęp do danych osobowych miało nieliczne grono osób, a efektywność procesów przetwarzania była niewielka. Sytuacja w tym zakresie uległa zmianie wskutek informatyzacji – zastosowanie komputerów i zautomatyzowanych metod przetwarzania danych w wielu dziedzinach, w tym również w administracji publicznej, spowodowało, że znacznie wzrosła ilość przetwarzanych danych, a dzięki połączeniu komputerów w sieci dostęp do danych stał się możliwy dla znacznie większej liczby osób, a także istotnie zwiększyła się efektywność procesów informacyjnych. Jednak tym – bez wątpienia korzystnym rezultatom, przyczyniającym się do poprawy sprawności działań administracji publicznej – towarzyszył również wzrost zagrożeń związanych z błędami przy przetwarzaniu danych, nieuprawnionym dostępem do danych, ich utratą, nieuprawnionym wykorzystaniem danych i innych niepożądanych skutków związanych ze zautomatyzowanym przetwarzaniem danych.

Konsekwencją zmiany charakteru przetwarzania danych i wynikających stąd zagrożeń jest konieczność zapewnienia osobom, których dane poddawane są przetwarzaniu, ochrony przed negatywnymi skutkami niezgodnego z prawem przetwarzania danych. Realizację tego celu mają umożliwić prawne regulacje z zakresu ochrony danych osobowych. Po-

trzebę tworzenia tego rodzaju regulacji dostrzeżono już w latach siedemdziesiątych XX w. w Europie Zachodniej, co zaowocowało pierwszymi ustawami dotyczącymi ochrony danych osobowych, których adresatami były organy administracji publicznej. W latach osiemdziesiątych i dziewięćdziesiątych XX w. stworzone zostały europejskie standardy prawne ochrony danych osobowych. W Polsce problematyka ta została uregulowana stosunkowo późno – w roku 1997. W kolejnych latach podjęte zostały wysiłki zmierzające do ujednolicenia przepisów w tym zakresie w Unii Europejskiej, przeprowadzono reformę, w wyniku której przyjęto przepisy mające bezpośrednie zastosowanie we wszystkich państwach członkowskich UE.

Przez ostatnie pięćdziesiąt lat ukształtowane zostały ramy prawne ochrony danych osobowych, jednak prawodawca unijny zdecydował się na jednolite ujęcie tej problematyki zarówno dla sektora publicznego, jak i prywatnego, w niewielkim tylko stopniu uznając szczególny charakter przetwarzania danych osobowych przez podmioty publiczne. Jednocześnie prawodawca unijny pozostawił państwom członkowskim możliwość uzupełnienia, ograniczenia lub odmiennego uregulowania prawnego konstrukcji z zakresu ochrony danych osobowych, po to, aby uwzględnić specyfikę przetwarzania danych osobowych w niektórych dziedzinach, w tym także w administracji. Polski prawodawca skorzystał z tej możliwości, przyjmując szczegółowe regulacje prawne, w których uregulowane zostały niektóre zagadnienia dotyczące ochrony danych osobowych w administracji publicznej. Jednakże pomimo rozbudowanej regulacji prawnej, przetwarzanie i ochrona danych osobowych w administracji publicznej napotyka wiele trudności i jest problematyką wzbudzającą liczne kontrowersje.

Występujące w obszarze działań administracji publicznej problemy z przetwarzaniem danych osobowych i spełnieniem obowiązków wynikających z przepisów o ochronie danych są powodem krytycznych opinii i ocen, a niekiedy nawet negowania potrzeby zapewnienia ochrony danych osobowych w administracji. Czasami uznaje się, że dotychczasowe przepisy proceduralne są wystarczające i zapewniają odpowiedni poziom ochrony, a co za tym idzie, kwestionuje się potrzebę istnienia szczegółowych regulacji i nakładania na organy administracji dodat-

kowych obowiązków. Jednak takie podejście nie uwzględnia postępu technicznego i konsekwencji, jakie z niego wynikają w zakresie zagrożeń dla prywatności osób, których dane poddawane są przetwarzaniu. W warunkach powszechnego wykorzystywania w administracji publicznej technologii informacyjnych konieczne jest zapewnienie ochrony na znacznie wyższym niż dotychczasowy poziomie. Niekiedy problemy wynikają z niewłaściwej interpretacji przepisów o ochronie danych, która prowadzi do nieuprawnionych wniosków (np. do powoływania się na potrzebę ochrony danych przy odmowie udostępnienia danych osobowych podmiotowi, który jest uprawniony do ich uzyskania, czy do sięgania po niewłaściwą podstawę przetwarzania danych, np. zgodę, gdy dopuszczalność przetwarzania danych wynika z przepisów prawa). Przyczyną „nadgorliwej" interpretacji (nadinterpretacji) tych przepisów bywa także obawa przed odpowiedzialnością w postaci administracyjnej kary pieniężnej za naruszenie przepisów o ochronie danych osobowych. Zdarza się również, że źródłem problemów jest niezrozumienie istoty ochrony danych osobowych oraz wynikające z tego przekonanie o konieczności ochrony samych danych, w oderwaniu od zasadniczego celu regulacji – ochrony osób, których dane dotyczą, przed negatywnymi konsekwencjami wynikającymi z niezgodnego z prawem przetwarzania danych.

Główną tezą badawczą pracy jest stwierdzenie, że prawodawca polski nie wykorzystał w pełni możliwości, jakie przewidziane zostały w przepisach unijnych, i tworząc szczególne przepisy krajowe, nie uwzględnił w wystarczającym stopniu specyfiki przetwarzania i ochrony danych osobowych w administracji publicznej. Konsekwencją takiego stanu rzeczy są liczne wątpliwości i problemy związane z interpretacją przepisów, jak też trudności z praktyczną realizacją wielu wymogów z zakresu ochrony danych osobowych w administracji publicznej.

Aby można było wykazać zasadność wskazanej powyżej tezy, konieczna jest realizacja pierwszego z celów badawczych pracy: przeprowadzenie analizy unijnych i krajowych przepisów dotyczących przetwarzania i ochrony danych osobowych w administracji publicznej oraz dokonanie oceny przyjętych rozwiązań prawnych. Kolejnym, nie mniej istotnym, celem rozprawy jest identyfikacja obszarów i zagadnień problematycz-

nych, przepisów, które nie są jednoznaczne i mogą być różnie interpretowane, oraz przedstawienie propozycji takiej wykładni tych przepisów, która pozwala w możliwie jak największym stopniu uwzględnić specyfikę administracji publicznej. Wreszcie tam, gdzie istniejące problemy nie są możliwe do rozwiązania przy pomocy wykładni, bądź gdzie specyfika administracji publicznej powinna zostać uwzględniona w większym zakresie, zostaną sformułowane wnioski *de lege ferenda* i propozycje innych działań, które mogą zostać podjęte w celu poprawy poziomu ochrony danych osobowych, przy jednoczesnym ograniczeniu obciążeń nakładanych na administrację publiczną.

Problematyka podjęta w niniejszej książce nie doczekała się dotąd wystarczającego opracowania w piśmiennictwie przedmiotu. W okresie kilku ubiegłych lat (od czasu przeprowadzenia unijnej reformy ochrony danych) ukazało się wiele publikacji dotyczących ochrony danych osobowych. Część z nich odnosi się do szeroko rozumianego sektora publicznego, brakuje jednak aktualnych i kompleksowych opracowań dotyczących przetwarzania i ochrony danych w administracji publicznej. Istniejące publikacje dotyczące sektora publicznego mają z reguły charakter ogólny i nie dotykają wielu zagadnień z zakresu przetwarzania danych osobowych w administracji publicznej, gdyż sektor publiczny jest rozległy, zróżnicowany i obejmuje także podmioty poddane odrębnej regulacji prawnej[1]. Nieliczne wyjątki w tym zakresie stanowią opracowania, które jednak dotyczą jedynie wybranych zagadnień związanych z ochroną danych osobowych w administracji[2]. Ponadto przeważająca większość publikacji odnoszących się do ochrony danych osobowych w sektorze publicznym ma charakter poradnikowy, natomiast brakuje

[1] Między innymi policję, prokuraturę, sądy i inne podmioty publiczne działające w obszarze zapobiegania, wykrywania i zwalczania przestępczości, co zostało uregulowane w dyrektywie 2016/680 i wdrażającej ją ustawie z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125).

[2] Na przykład: M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018; M. Sakowska-Baryła, *Specyfika stosowania RODO przez organy i podmioty publiczne* [w:] *Aktualne problemy prawnej ochrony danych osobowych 2020*, red. G. Sibiga, dodatek specjalny do MoP 2020/23, s. 27–34.

opracowań naukowych, zawierających analizy teoretyczne i konstrukcyjne, w których przykłady nie stanowią głównej treści, a są jedynie ilustracją dla zasadniczych wywodów. W tym zakresie niniejsze opracowanie – w zamierzeniu autora – ma wypełnić istniejącą lukę w literaturze przedmiotu i stanowić wkład w rozwój badań naukowych nad problematyką ochrony danych osobowych w administracji publicznej.

Warto również wspomnieć o opracowaniach z tego zakresu, które ukazały się jeszcze na gruncie poprzednich przepisów o ochronie danych, odnoszących się głównie do postępowania administracyjnego[3]. Pomimo upływu lat i zmiany przepisów te wartościowe publikacje nadal mogą być wykorzystywane w zakresie, w jakim obecne regulacje stanowią kontynuację dotychczasowych rozwiązań prawnych. Jednakże zagadnienia związane z ochroną danych osobowych w administracji publicznej nie ograniczają się do kwestii proceduralnych, obejmują również wiele zagadnień z zakresu prawa materialnego, dlatego konieczne jest prowadzenie badań nad tą problematyką w szerszym wymiarze.

Przy pisaniu tej książki wykorzystane zostaną różnorodne materiały źródłowe. Podstawę do przeprowadzenia analiz stanowić będą akty normatywne, zarówno prawa unijnego, jak i krajowego. Mają one pozwolić na ukazanie obecnego stanu prawnego, który powinien być punktem odniesienia dla organów administracji, na których spoczywa obowiązek przetwarzania i ochrony danych osobowych. Istotną rolę przy dokonywaniu wykładni przepisów odgrywają orzeczenia sądów oraz decyzje organu nadzorczego. W opracowaniu uwzględnione zostaną także publikacje naukowe oraz komentarze do przepisów, jak również inne źródła, których szczegółowy wykaz zostanie zamieszczony w końcowej części pracy.

Niniejsza książka składa się ze wstępu, dziesięciu rozdziałów merytorycznych oraz zakończenia. W rozdziale I omówione zostaną zagadnienia ogólne dotyczące ochrony danych osobowych w administracji

[3] P. Litwiński, *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, Warszawa 2009; G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003.

publicznej – przedstawiona zostanie geneza, specyfika i regulacja prawna w tej dziedzinie. Analiza tej problematyki ma pozwolić na ukazanie powodów wprowadzenia, istoty i celów prawnej regulacji ochrony danych osobowych, wskazanie charakterystycznych cech przetwarzania danych osobowych w administracji publicznej, które uzasadniają uwzględnienie specyfiki działań administracji w przepisach, oraz zarysowanie złożonego kształtu obecnych regulacji prawnych w omawianym zakresie. W rozdziale II zawarte zostaną analizy odnoszące się do wyjaśnienia podstawowych pojęć i konstrukcji prawnych z zakresu ochrony danych osobowych. Potrzeba przedstawienia pojęć wynika z odmiennego znaczenia, jakie niektórym pojęciom nadał prawodawca, bądź z wątpliwości związanych z ich interpretacją. W tej części opracowania omówione zostaną pojęcia: danych osobowych, przetwarzania danych, zbioru danych, administratora, współadministratora i podmiotu przetwarzającego, a także inspektora ochrony danych, organu nadzorczego i zabezpieczenia danych. Rozdział III dotyczył będzie realizacji zasad przetwarzania danych osobowych w administracji publicznej. W rozdziale tym omówione zostaną normy, które prawodawca unijny uznał za najistotniejsze i podniósł do rangi zasad ogólnych. Są one szczególnie istotne w procesach przetwarzania danych, a wszelkie działania podejmowane na danych osobowych powinny być zgodne z tymi zasadami. Uzupełnieniem katalogu zasad ogólnych jest wymóg rozliczalności i wskazanie administratora jako podmiotu, na którym spoczywa odpowiedzialność za przestrzeganie zasad. W kolejnym rozdziale analizie poddane zostaną podstawy dopuszczalności przetwarzania danych osobowych, czyli przesłanki, na których administrator może opierać przetwarzanie danych. Jest to jedna z podstawowych kwestii, której znaczenie praktyczne jest również istotne w administracji. Niektóre z podstaw dopuszczalności przetwarzania powinny być uznane za typowe i właściwe dla organów administracji (np. realizacja obowiązku wynikającego z przepisu prawa), natomiast inne (np. zgoda) powinny być wykorzystywane wyjątkowo, jako że z oparciem przetwarzania na ich podstawie mogą wiązać się poważne wątpliwości i problemy. Przedmiotem rozważań w rozdziale V będzie realizacja praw osób, których dane dotyczą, przez organy administracji publicznej. W ramach tego rozdziału przedstawiona zostanie klasyfikacja uprawnień podmiotów danych, a następnie zostaną omówione poszczególne grupy uprawnień

i wskazane zostaną ograniczenia poszczególnych praw przyznanych osobom, których dane dotyczą. Także w tym zakresie ukazana zostanie specyfika przetwarzania danych osobowych w administracji i konsekwencje, które z niej wynikają (np. niemożność realizacji „prawa do bycia zapomnianym" w sytuacji, gdy organ administracji publicznej przetwarza dane osobowe, gdy jest to konieczne do wywiązania się z obowiązku wynikającego z przepisu prawa). Rozdział VI dotyczyć będzie obowiązków administratora i podmiotu przetwarzającego dane osobowe w administracji publicznej. W tej części monografii przedstawiona zostanie klasyfikacja obowiązków, a następnie omówione zostaną poszczególne grupy wymogów ciążących na organach administracji przetwarzających dane osobowe. W ramach tych rozważań wskazane zostaną nie tylko konstrukcje prawne określające obowiązki, ale także praktyczny wymiar ich realizacji oraz liczne wątpliwości, jakie pojawiają się przy interpretacji i stosowaniu przepisów. Istotną częścią tych analiz będzie wskazanie ograniczeń i wyjątków oraz zasygnalizowanie potrzeby dokonania zmian przepisów, tak aby ograniczyć uciążliwość spełnienia obowiązków przez organy administracji publicznej. W rozdziale VII analizie zostaną poddane przepisy dotyczące powołania, statusu i zadań inspektora ochrony danych – osoby, która ma zapewnić merytoryczne wsparcie dla administratora w obszarze ochrony danych osobowych i może odgrywać szczególną rolę w strukturach administracji publicznej. Rozdział VIII będzie zawierał omówienie zagadnień związanych z nadzorem nad przetwarzaniem i ochroną danych osobowych w administracji publicznej, jaki sprawuje Prezes Urzędu Ochrony Danych Osobowych. Zawarte w tym rozdziale analizy będą odnosić się do pozycji i statusu organu nadzorczego, jego zadań i uprawnień oraz kontroli zgodności przetwarzania danych z prawem, postępowania w sprawie naruszenia ochrony danych, a także form nadzorczego oddziaływania organu, w tym nakładania administracyjnych kar pieniężnych. W rozdziale IX zostanie omówiona problematyka odpowiedzialności za niezgodne z prawem przetwarzanie danych osobowych w administracji publicznej, w tym odpowiedzialności administracyjnej, cywilnej, porządkowej i dyscyplinarnej oraz karnej. Rozdział X pracy zostanie poświęcony omówieniu wybranych zagadnień szczegółowych z zakresu ochrony danych osobowych w administracji publicznej, które budzą wiele wątpliwości i problemów praktycznych. Wśród tych zagadnień

przedstawione zostaną analizy odnoszące się do relacji ochrony danych osobowych i dostępu do informacji publicznej, jawności informacji w rejestrach publicznych, monitoringu, realizacji projektów finansowanych ze środków unijnych oraz telepracy i pracy zdalnej.

Ostatnią merytoryczną część książki stanowić będzie zakończenie, w którym zawarte zostanie podsumowanie i przedstawione zostaną najistotniejsze wnioski płynące z przeprowadzonych badań.

Podstawowym zamierzeniem autora niniejszej monografii jest poszukiwanie optymalnego modelu ochrony danych osobowych w administracji publicznej. Można wyrazić nadzieję, że to opracowanie stanowić będzie impuls do podejmowania pogłębionych badań nad omawianą problematyką, a zarazem głos w dyskusji nad potrzebą i kształtem ochrony danych osobowych w administracji publicznej.

W pracy uwzględniony został stan prawny na dzień 30.06.2021 r.

Paweł Fajgielski

Rozdział I

OCHRONA DANYCH OSOBOWYCH W ADMINISTRACJI PUBLICZNEJ – GENEZA, SPECYFIKA I REGULACJA PRAWNA

1. Wprowadzenie

Ochrona danych osobowych to dziedzina stosunkowo młoda – liczy sobie zaledwie pół wieku, a w Polsce problematyka ta jest przedmiotem regulacji prawnej od ponad dwudziestu lat (od roku 1997). Przez wiele lat gromadzenie i wykorzystywanie informacji w administracji publicznej było uregulowane w sposób bardzo ogólny, w przepisach nie było szczegółowych norm odnoszących się do ochrony osób, których dane poddawane są przetwarzaniu, uprawnień tych osób ani obowiązków podmiotów, które przetwarzają dane. Jednak przemiany ustrojowe, ubieganie się o członkostwo w Unii Europejskiej oraz postęp techniczny sprawiły, że konieczne stało się prawne uregulowanie problematyki ochrony danych osobowych. Swobody gromadzenia i wykorzystywania danych osobowych w administracji, a także nastawienia, aby gromadzić wszelkie informacje, gdyż kiedyś mogą się one przydać, nie dało się pogodzić ze standardami demokratycznego państwa prawnego, zgodnie z którymi organy administracji powinny działać na podstawie i w granicach prawem określonych oraz gromadzić jedynie informacje, które są niezbędne dla realizacji zadań publicznych. Ochrona danych osobowych uznawana jest również za jeden z unijnych standardów prawnych,

dlatego państwa ubiegające się o członkostwo miały obowiązek dostosować swoje ustawodawstwo do unijnych przepisów o ochronie danych. Także gwałtowny postęp techniczny, który przyczynił się do znacznego ułatwienia gromadzenia, przetwarzania, przesyłania i udostępniania danych pociągnął za sobą potrzebę wprowadzenia regulacji prawnych określających wymogi dotyczące przetwarzania danych oraz pozwalających na zapewnienie ochrony osobom, których dane poddawane są przetwarzaniu.

Dla zrozumienia istoty prawnej regulacji ochrony danych osobowych konieczne wydaje się przedstawienie genezy tej problematyki. Pozwoli ona nie tylko ukazać powody wprowadzenia przepisów, ale także wyjaśnić rolę, jaką odgrywają one w działaniach administracji publicznej. W niniejszym rozdziale omówiona zostanie także specyfika ochrony danych osobowych w administracji, wskazane zostaną cechy, które odróżniają przetwarzanie danych przez administrację od przetwarzania danych przez podmioty prywatne oraz konsekwencje, jakie z tego wynikają. Wśród zagadnień ogólnych, wprowadzających do bardziej szczegółowych analiz, nie powinno zabraknąć omówienia konstytucyjnych aspektów przetwarzania i ochrony danych przez administrację publiczną. Kolejna część niniejszego rozdziału zawiera przedstawienie prawnej regulacji ochrony danych osobowych w administracji publicznej, a więc przepisów, które normują tę problematykę, gdyż regulacja w omawianym obszarze jest złożona i składa się zarówno z przepisów prawa unijnego, jak i z krajowych aktów normatywnych.

2. Geneza ochrony danych osobowych w administracji publicznej

Administracja publiczna opiera swoje działania na informacjach, ich gromadzenie i wykorzystywanie jest konieczne dla jej funkcjonowania i realizacji zadań publicznych. Administracja tworzy również i udostępnia określone informacje innym podmiotom[1].

[1] Szerzej na temat procesów informacyjnych w administracji publicznej por. P. Fajgielski, *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania*

W rozległych zasobach informacyjnych administracji publicznej szczególnie istotne znaczenie mają informacje dotyczące osób fizycznych określane mianem danych osobowych. Przetwarzanie tego rodzaju informacji jest niezbędne, gdyż podstawowym obszarem aktywności administracji jest załatwianie spraw indywidualnych. Bez zgromadzenia informacji o osobach organ administracji nie jest zazwyczaj w stanie załatwić spraw osób, których informacje te dotyczą.

Przez wiele lat informacje[2] były przetwarzane w administracji publicznej w sposób tradycyjny (ręcznie), na nośnikach papierowych, w różnego rodzaju dokumentach, aktach, kartotekach i ewidencjach. Gromadzenie i wykorzystywanie informacji w ten sposób było kosztowne, czasochłonne i pracochłonne, pozwalało na zebranie niewielkiego zasobu informacji. Stosunkowo niewielka skala przetwarzania danych sprawiała, że za wystarczające uznawano wówczas regulacje prawne określające procedury postępowania administracyjnego, natomiast nie dostrzegano konieczności uregulowania procesów przetwarzania danych. Jednakże już na tym etapie rozwoju procesów informacyjnych pojawiały się problemy z przetwarzaniem informacji w różnego rodzaju kartotekach i ewidencjach – przy braku regulacji prawnych w tym zakresie informacje były gromadzone w sposób dowolny, z różnych źródeł, często bez weryfikacji ich prawdziwości, jak również bez wiedzy osób, których informacje te dotyczyły. Taki stan rzeczy prowadził niekiedy do sytuacji,

i ochrony, Wrocław 2007.

[2] W niniejszym opracowaniu określenia „informacje" i „dane" będą wykorzystywane zamiennie i traktowane jako równoznaczne w znaczeniu prawnym. Autor ma świadomość, iż takie ujęcie stanowi uproszczenie, gdyż określenia te na gruncie różnych obszarów badawczych mają nieco odmienne zakresy znaczeniowe (ściślej rzecz ujmując, informacja zawiera treść poznawczą, natomiast dane to informacje zapisane przy pomocy określonej konwencji znaczeniowej). Na problem ten zwrócono uwagę w literaturze przedmiotu – por. G. Szpor, *Pojęcie informacji a zakres danych osobowych* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, red. P. Fajgielski, Lublin 2008, s. 7 i n. Jednakże prawodawca posługuje się tymi określeniami zamiennie, uznając je za synonimy (stwierdzając, że dane osobowe to informacje o osobach), dlatego też wskazane powyżej uproszczenie wydaje się prawnie uzasadnione.

gdy zgromadzone dane były nieprawidłowe, a osoby, których te dane dotyczyły, nie miały możliwości ich sprawdzenia i skorygowania[3].

Aby poprawić efektywność procesów informacyjnych w administracji publicznej (podobnie jak w innych obszarach życia społecznego i gospodarczego), podejmowane były działania zmierzające do wykorzystania różnorodnych urządzeń technicznych. Wysiłki w tym zakresie miały wpływ na zwiększenie wydajności przetwarzania danych. Sytuacja zaczęła się bardziej dynamicznie zmieniać w drugiej połowie XX w., kiedy to w administracji rozpoczęto stosowanie zautomatyzowanych technik przetwarzania danych. Upowszechnienie wykorzystywania komputerów w administracji pozwoliło usprawnić i przyspieszyć wykonywanie wielu operacji, których przedmiotem są informacje, w tym także dane osobowe, spowodowało znaczne zwiększenie możliwości administracji w zakresie zarówno ilości gromadzonych danych, jak też możliwości ich automatycznego przetwarzania.

Jednak wdrażanie w administracji publicznej technologii informatycznych pociągnęło za sobą nasilenie się wskazanych powyżej zagrożeń związanych z gromadzeniem danych osobowych, a także pojawienie się wielu nowych zagrożeń, które dotyczyły sposobów przetwarzania danych i wykorzystywania informacji. Zastosowanie komputerów sprawiło, że znacznie zwiększyła się ilość przetwarzanych danych, informacje zawarte w różnych bazach danych mogły być ze sobą zestawiane i łączone (przy wykorzystaniu uniwersalnych identyfikatorów osobowych, takich jak np. numer PESEL). Informacje przetwarzane komputerowo dostępne były dla coraz szerszego kręgu osób, ułatwione stało się ich kopiowanie, co pociągało za sobą większe zagrożenie polegające na bezprawnym wykorzystywaniu danych. Ponadto automatyzacja procesów przetwarzania danych ułatwiała prowadzenie w sposób niejawny analizy aktywności osób i tworzenie tzw. profili osobowościowych, które mogą prowadzić do naruszania praw osób, których zgromadzone dane dotyczą. Zagrożenia te zaczęły być postrzegane jako ryzyko bezprawnej ingerencji w sferę prywatności. W literaturze przedmiotu powszechnie

[3] Por. A. Mrózek, *Ustawowe prawo ochrony danych – analiza prawnoporównawcza*, Toruń 1981, s. 10.

uznaje się, że ochrona danych osobowych wywodzi się z konstrukcji prawa do prywatności[4].

Gromadzenie i wykorzystywanie danych osobowych przez administrację publiczną nieuchronnie wiąże się z wkraczaniem organów w sferę prywatności osób fizycznych. Prywatność rozumiana szeroko, jako „prawo do bycia pozostawionym w spokoju"[5], definiowana również jako „prawo jednostki do życia swym własnym życiem, układanym według własnej woli, z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej"[6], a ujmowana w kontekście przetwarzania danych jako „roszczenie jednostek (...) do samodzielnego decydowania kiedy, jak i w jakim zakresie informacje o nich są komunikowane innym"[7], była uznawana przez prawodawców w wielu krajach za dobro zasługujące na ochronę od początku XX w.[8]

Potrzeba zbierania danych osobowych przez administrację publiczną zasadniczo nie była kwestionowana, powszechnie uznawano, że z uwagi na konieczność przetwarzania danych dla realizacji zadań publicznych, prawo do prywatności powinno w tym zakresie podlegać ograniczeniu. Przez wiele lat procesy przetwarzania danych nie były poddawane regulacji prawnej, co w warunkach automatyzacji tych działań coraz częściej było źródłem różnego rodzaju wątpliwości i problemów.

Ochrona prywatności przez kilkadziesiąt lat XX wieku realizowana była na płaszczyźnie cywilnoprawnej poprzez wykorzystanie konstrukcji ochrony dóbr osobistych. Jednak ochrona tego rodzaju miała przede

[4] Por. M. Sakowska-Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2015, s. 23 i wskazaną tam literaturę.

[5] S.D. Warren, L.D. Brandeis, *The Right to Privacy*, „Harvard Law Review" 1890/4, s. 193–220.

[6] A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego. Zagadnienia konstrukcyjne*, „Studia Cywilistyczne" 1972/20, s. 30.

[7] A.F. Westin, *Privacy and Freedom*, New York 1967, s. 7.

[8] Szerzej na temat różnych koncepcji prywatności i prawa do prywatności por. m.in. F.H. Cate, *Privacy in the Information Age*, Washington 1997, s. 19–23, w literaturze polskiej m.in. K. Motyka, *Spory wokół prawa do prywatności na przykładzie Stanów Zjednoczonych* [w:] *Prawo do prywatności. Aspekty prawne i psychologiczne*, red. K. Motyka, Lublin 2001, s. 9–46.

wszystkim charakter następczy – mogła być realizowana w kontekście przetwarzania danych dopiero w sytuacji, gdy nastąpiło naruszenie, a roszczenia cywilnoprawne z tytułu naruszenia prywatności były kierowane do organów administracji publicznej niezwykle rzadko. Wdrażanie technik zautomatyzowanego przetwarzania danych osobowych, zarówno w sektorze publicznym, jak i w sektorze prywatnym uwidoczniło potrzebę zagwarantowania ochrony o charakterze prewencyjnym – stworzenia konstrukcji prawnych, które pozwolą chronić osoby przed negatywnymi konsekwencjami przetwarzania danych, a nie tylko reagować w sytuacji, gdy doszło już do naruszenia ich sfery prywatności.

W krajach Europy Zachodniej oraz w USA w latach sześćdziesiątych XX w. podjęta została dyskusja nad zasadnością uregulowania prawnego zautomatyzowanych procesów przetwarzania danych osobowych. Odpowiedzią prawodawcy na wskazane powyżej zagrożenia i potrzeby było stworzenie regulacji prawnych mających na celu ochronę osób, których dane dotyczą, przed negatywnymi konsekwencjami zautomatyzowanego przetwarzania danych (skrótowo określanych mianem przepisów o ochronie danych osobowych).

Pierwszą na świecie ustawą o ochronie danych była ustawa uchwalona w roku 1970 w jednym z niemieckich krajów związkowych – w Hesji[9]. Ta krótka (licząca 17 paragrafów) regulacja prawna adresowana była do podmiotów publicznych (głównie do administracji tego kraju związkowego) i dotyczyła maszynowego przetwarzania danych osobowych. Prawodawca nałożył w niej między innymi wymóg uniemożliwienia dostępu do danych osobom nieuprawnionym, wymóg należytego zabezpieczenia danych oraz obowiązek zachowania danych w tajemnicy przez osoby przetwarzające. W heskiej ustawie o ochronie danych zagwarantowano również osobom, których dane dotyczą, uprawnienia do żądania poprawienia danych nieprawidłowych oraz żądania zapewnienia ochrony przed naruszeniami wynikającymi z bezprawnego przetwarzania danych. W ustawie zapisano, że w przypadku baz danych i systemów informatycznych należy zagwarantować, aby żaden organ nie mógł

[9] Ustawa o ochronie danych Hesji, *Datenschutzgesetz vom 7. Oktober 1970*, Gesetz- und Verordnungsblatt für das Land Hessen, I. S. 625.

przeglądać ani pobierać dokumentów i danych, do których na podstawie swojej właściwości nie jest uprawniony. Prawodawca heski przewidział powołanie organu nadzorczego – pełnomocnika landowego, który miał nadzorować przestrzeganie przepisów o ochronie danych, zapewniając osobom, których dane dotyczą, prawo zwrócenia się do pełnomocnika w przypadku podejrzenia naruszenia ich praw w związku z przetwarzaniem danych. Za wykroczenie porządkowe uznano udostępnianie danych osobom nieuprawnionym.

Pierwszą ogólnokrajową ustawą regulującą problematykę ochrony danych była szwedzka ustawa o danych z 13.05.1973 r.[10] Uchwalenie tej ustawy było efektem debaty publicznej dotyczącej możliwości wykorzystania danych o warunkach życia i postawach ludności przez państwo, którą zapoczątkował spis powszechny ludności i mieszkań. W ramach debaty zwracano uwagę na to, że rozwój technologii automatycznego przetwarzania danych w połączeniu z numerem identyfikacyjnym nadawanym osobom daje administracji publicznej rozległe możliwości krzyżowego sprawdzania informacji osobowych w różnych rejestrach, co pociąga za sobą konieczność wprowadzenia ograniczeń w tym zakresie[11]. Cechą charakterystyczną szwedzkiej regulacji prawnej było uzależnienie możliwości tworzenia zbiorów danych osobowych od uprzedniego uzyskania zezwolenia organu nadzorczego.

W kolejnych latach uchwalono ustawy regulujące problematykę ochrony danych osobowych w większości państw Europy Zachodniej[12]. Wspomniane powyżej akty normatywne nie były ograniczone do regulacji przetwarzania danych przez instytucje publiczne, lecz dotyczyły również sektora prywatnego, większość ustaw normowało zagadnienia te

[10] Szwedzka ustawa o danych, *Datalag*, Svensk författningssamling [SFS] 1973:289. Na temat tej ustawy por. J. Kosik, *Ochrona jednostki w prawie szwedzkim przed zastosowaniem komputerów*, PiP 1975/6, s. 111–121.

[11] Por. A. Paulsson, *The welfare state that wanted to keep track of its citizens: personal identity numbers as administrative technology* [w:] *Modernizing the Public Sector: Scandinavian Perspectives*, ed. by I. Lapsley, H. Knutsson, London–New York 2017, s. 92–93.

[12] Między innymi w: Republice Federalnej Niemiec, we Francji, w Austrii, Danii, Norwegii i Luksemburgu. Szerzej na ten temat w polskiej literaturze przedmiotu pisał A. Mrózek, *Ustawowe...*, s. 61 i n.

w sposób niemal jednolity. Jednak na przykład niemiecka federalna ustawa o ochronie danych[13] z roku 1977 regulowała te kwestie odrębnie; podzielona była na część odnoszącą się do przetwarzania danych przez podmioty publiczne (administrację federalną) oraz część dotyczącą przetwarzania danych przez podmioty prywatne.

Warto wspomnieć także o prawnej regulacji ochrony danych osobowych w Stanach Zjednoczonych Ameryki Północnej, zawartej w ustawie „o ochronie praw osobistych przed naruszeniami poprzez wykorzystanie federalnych rejestrów danych, o zabezpieczeniu jednostce dostępu do zbiorów danych wykorzystywanych przez organy federalne i o powołaniu Komisji Badawczej w Zakresie Ochrony Praw Osobistych", określanej skrótowo mianem *PrivacyAct of 1974*[14]. Ustawa ta reguluje zasady gromadzenia, przechowywania, wykorzystywania i udostępniania informacji o osobach przez agencje federalne. Jest to o tyle istotne, że w USA do dziś nie wprowadzono ogólnej regulacji prawnej normującej całościowo problematykę ochrony danych osobowych przez podmioty prywatne[15].

W odróżnieniu od państw Europy Zachodniej i USA, gdzie wdrażano nowoczesne technologie informatyczne w administracji publicznej, a wprowadzenie prawnych mechanizmów ochrony osób w związku z przetwarzaniem danych uznawano za istotny element państwa demokratycznego, w Europie Środkowej i Wschodniej w latach siedemdziesiątych XX w. nie uchwalono przepisów dotyczących ochrony danych osobowych. Złożyło się na to kilka powodów. Przede wszystkim w państwach dawnego bloku socjalistycznego sprawowanie rządów opierało się w znacznym stopniu na kontroli aparatu państwowego nad obywatelami, a praktycznie nieograniczona możność swobodnego pozy-

[13] Niemiecka federalna ustawa o ochronie danych z roku 1977, *Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG) vom 27.01.1977*, Bundesgesetzblatt 1977, Teil I Nr. 7, s. 201.

[14] Amerykańska ustawa o prywatności, *Privacy Act of 1974*, 5 USC § 552a.

[15] Szerzej na temat amerykańskiego podejścia do ochrony danych osobowych por. B. Marcinkowski, *Dane osobowe: Polska – UE – USA. Współczesne wyzwania. Administracyjnoprawne zagadnienia odpowiedniości poziomu ochrony danych osobowych na przykładzie amerykańskiego prawa federalnego*, Warszawa 2018, s. 127 i n.

skiwania i wykorzystywania informacji o obywatelach stanowiła ważne narzędzie umożliwiające realizację tego celu. Informacje o obywatelach były masowo gromadzone i wykorzystywane nie tylko w celach centralnego planowania i administrowania, ale także między innymi w celu inwigilacji osób i zwalczania opozycji. W tym stanie rzeczy rządzący nie byli zainteresowani wprowadzeniem regulacji prawnych, które zawierałyby ograniczenia dotyczące zakresu i sposobu przetwarzania danych osobowych. Kolejnym powodem, który sprawiał, że w zasadzie nie podejmowano w tamtym czasie szerszej dyskusji nad potrzebą prawnej regulacji ochrony danych, był stosunkowo niski poziom wykorzystywania komputerów i zautomatyzowanych metod przetwarzania danych w administracji publicznej.

Działania zmierzające do prawnego uregulowania problematyki ochrony osób fizycznych w związku z przetwarzaniem danych osobowych podejmowane były również na płaszczyźnie międzynarodowej. Dla administracji publicznej istotne znaczenie miało wydanie przez Radę Europy w roku 1974 Rezolucji nr (74) 29 w sprawie ochrony prywatności osób fizycznych w kontekście elektronicznych banków danych w sektorze publicznym[16]. W rezolucji zwrócono uwagę na potrzebę ochrony prywatności w związku z wykorzystywaniem przez władze publiczne elektronicznych banków danych osobowych. W załączniku do rezolucji wyjaśniono pojęcia „informacje dotyczące osób" i „elektroniczne banki danych" oraz sformułowano osiem podstawowych zasad dotyczących gromadzenia informacji dotyczących osób w elektronicznych bankach danych prowadzonych w sektorze publicznym. Jako pierwszą zasadę wskazano wymóg regularnego informowania opinii publicznej o tworzeniu, funkcjonowaniu i rozwijaniu elektronicznych banków danych w sektorze publicznym. Druga zasada odnosiła się do gromadzonych informacji – powinny one być uzyskiwane zgodnie z prawem i uczciwie, być ścisłe i aktualne oraz adekwatne i odpowiednie do celów, w któ-

[16] Rezolucja Rady Europy nr (74) 29, *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*, z 20.09.1974 r., tekst rezolucji dostępny na oficjalnej stronie Rady Europy: https://www.coe.int; polski przekład [w:] T. Jasudowicz, *Ochrona danych. Standardy europejskie. Zbiór materiałów*, Toruń 1998, s. 31–33.

rych zostały zgromadzone. Ponadto wskazano, iż należy dołożyć starań w celu skorygowania informacji nieścisłych oraz usunięcia informacji niewłaściwych, nieistotnych oraz zbędnych. W myśl trzeciej zasady – w szczególności gdy w elektronicznych bankach danych wykorzystywane są informacje dotyczące intymnej sfery życia osób albo wykorzystanie tego rodzaju informacji może stanowić źródło dyskryminacji – istnienie takich banków danych powinno być przewidziane w ustawie albo innej regulacji prawnej bądź ogłoszone publicznie w formie dokumentu zgodnie z systemem prawnym danego państwa członkowskiego. W tego rodzaju regulacjach prawnych lub dokumentach powinny zostać sprecyzowane cele gromadzenia i wykorzystywania informacji oraz warunki ich udostępniania. Zgromadzonych informacji nie wolno wykorzystywać w celach innych niż określone w regulacji prawnej lub dokumencie, chyba że przewidziano w tym zakresie wyraźny wyjątek. Zgodnie z czwartą zasadą należy ustanowić reguły określające czas, po upływie którego zgromadzone informacje nie będą mogły być przechowywane ani wykorzystywane. Odstępstwa od tej zasady mogą jednak dotyczyć wykorzystywania informacji do celów statystycznych, naukowych lub historycznych. Piąta zasada przewiduje przyznanie każdej osobie prawa uzyskania informacji o tym, jakie dane na jej temat zostały zgromadzone. Ograniczenia i wyjątki od tej zasady powinny być ściśle uregulowane. Szósta zasada odnosi się do konieczności podjęcia środków zapobiegających nadużyciom lub niedozwolonemu wykorzystywaniu danych. Do środków tego rodzaju zaliczono nałożenie na osoby dokonujące operacji na elektronicznych bankach danych obowiązku zachowania tajemnicy przetwarzanych informacji oraz wyposażenie elektronicznych banków danych w zabezpieczenia uniemożliwiające osobom nieuprawnionym dostęp do informacji oraz umożliwiające wykrywanie świadomych lub nieświadomych zniekształceń informacji. Siódma zasada nakazuje, aby dostęp do informacji, które nie mogą być swobodnie udostępniane opinii publicznej, był ograniczony do osób uprawnionych ze względu na wykonywane przez nie obowiązki. Ostatnia – ósma zasada stanowi, że dane osobowe wykorzystywane do celów statystycznych nie mogą być rozpowszechniane, chyba że w sposób uniemożliwiający powiązanie tego rodzaju danych z określoną osobą. Zasady te zachowują aktualność do dziś. Przedstawiona powyżej rezolucja nie miała jednak charakteru prawnie wiążącego dla państw członkowskich Rady Europy, zawierała

jedynie zalecenie podjęcia środków koniecznych do zapewnienia realizacji zasad w niej sformułowanych[17].

Rozbieżności występujące między regulacjami prawnymi obowiązującymi w różnych państwach spowodowały podjęcie prac nad regulacją międzynarodową, która miałaby charakter wiążący i przyczyniłaby się do ujednolicenia przepisów o ochronie danych osobowych. Taką regulacją była przyjęta przez Radę Europy Konwencja nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[18], sporządzona w Strasburgu 28.01.1981 r. W konwencji 108 zdefiniowano podstawowe pojęcia, w tym pojęcie administratora zbioru danych, za którego w świetle przepisu uznano między innymi „władzę publiczną, agencję lub każdy inny organ właściwy na podstawie prawa wewnętrznego do określenia celu, któremu ma służyć zautomatyzowany zbiór danych, kategorii gromadzonych danych osobowych oraz sposobu przetwarzania, jakiemu dane będą poddawane" (art. 2 lit. d konwencji 108). Konwencja zasadniczo odnosi się jedynie do przetwarzania zautomatyzowanego, natomiast państwa, które ją ratyfikowały, mogą rozszerzyć zakres jej oddziaływania na niezautomatyzowane przetwarzanie danych. W konwencji sformułowano podstawowe zasady ochrony danych, w sposób zbliżony do reguł określonych w omówionej powyżej rezolucji nr (74) 29, ujmując je jako wymogi dotyczące: ograniczenia zbierania danych; jakości danych; określenia celu; ograniczenia wykorzystywania danych; zabezpieczenia danych; zagwarantowania osobom, których dane dotyczą, uprawnień do uzyskania informacji, korygowania danych, żądania usunięcia danych zgromadzonych bez-

[17] Podobne zasady określone zostały w innych niewiążących aktach międzynarodowych dotyczących ochrony danych wydanych przez: OECD – Wytyczne w sprawie ochrony prywatności i przepływu danych osobowych przez granice, 23.09.1980 r., *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, https://www.oecd.org/sti/ieconomy/ oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (dostęp: 20.12.2020 r.) oraz ONZ – Wytyczne w sprawie skomputeryzowanych zbiorów danych osobowych, *Guidelines for the Regulation of Computerized Personal Data Files*, G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989), https://digitallibrary.un.org/record/43365 (dostęp: 20.12.2020 r.).

[18] Konwencja nr 108 Rady Europy sporządzona w Strasburgu 28.01.1981 r., Dz.U. z 2003 r. Nr 3, poz. 25 z uzup.

prawnie, wniesienia skargi do organu nadzorczego oraz ograniczenia czasu przechowywania danych. W konwencji przewidziano również możliwość wprowadzenia w przepisach krajowych wyłączeń i ograniczeń w zakresie ochrony danych oraz nałożono na państwa członkowskie obowiązek wprowadzenia w prawodawstwie krajowym sankcji za naruszenie przepisów o ochronie danych. Konwencja 108 zawiera określenie minimalnego europejskiego standardu ochrony i miała stanowić wskazanie dla państw wprowadzających odpowiednie przepisy do swojego ustawodawstwa[19]. Uzupełnieniem konwencji 108 są liczne rekomendacje (zalecenia) sektorowe, uwzględniające specyfikę określonych dziedzin, w których przetwarzanie danych pociąga za sobą zwiększone zagrożenie dla prywatności. Jedna z rekomendacji odnosi się do przekazywania osobom trzecim danych osobowych będących w dyspozycji instytucji publicznych[20]. W rekomendacji tej wskazano między innymi sytuacje, w których dopuszczalne jest przekazywanie przez organy publiczne danych osobowych osobom trzecim (gdy jest to przewidziane prawem; gdy dane są powszechnie dostępne; gdy przekazanie jest zgodne z prawodawstwem wewnętrznym dotyczącym ochrony danych albo gdy osoba, której dane dotyczą, wyraziła na to zgodę). Ponadto w rekomendacji podkreślono wymóg informowania osób o tym, czy podanie danych jest obowiązkowe, czy dobrowolne; wskazano, że

[19] Szerzej na temat europejskich standardów ochrony danych osobowych por. m.in. M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010 i wskazaną tam literaturę. Zob. również: A. Mednis, *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej*, PiP 1997/6, s. 29 i n.; M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej. Transfer danych osobowych z Unii Europejskiej ze szczególnym uwzględnieniem transferu do Stanów Zjednoczonych w obecnym i nadchodzącym stanie prawnym*, Warszawa 2014. Warto wspomnieć również o tym, że konwencja 108 została w 2018 r. uzupełniona o protokół zmieniający, dzięki czemu została częściowo dostosowana do rozporządzenia 2016/679. Na ten temat zob.: M. Ciechomska, *Zmiana Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych*, MoP 2017/16, s. 871–877.

[20] Rekomendacja R (91) 10 z 9.09.1991 r. dotycząca przekazywania osobom trzecim danych osobowych będących w dyspozycji instytucji publicznych. Polskie tłumaczenie tej rekomendacji zawarte zostało w opracowaniu A. Mednisa, *Prawna ochrona danych osobowych*, Warszawa 1995, s. 73–78. Teksty wszystkich rekomendacji dostępne są na oficjalnej stronie internetowej Rady Europy poświęconej ochronie danych: https://www.coe.int/en/web/data-protection/.

łączenie baz danych posiadanych przez osoby trzecie z bazami danych organów publicznych powinno być zabronione, chyba że prawo krajowe wyraźnie na to zezwala, przewidując odpowiednie gwarancje ochrony praw osób, których dane dotyczą.

Wbrew intencjom prawodawcy ratyfikacja konwencji 108 przez większość państw europejskich nie pozwoliła na osiągnięcie zamierzonego celu, jakim było ujednolicenie krajowych regulacji prawnych w obszarze ochrony danych. Było to coraz bardziej problematyczne z uwagi na dążenie do stworzenia jednolitego europejskiego rynku, gdyż zróżnicowanie prawne dotyczące ochrony danych stanowiło przeszkodę w swobodnym przekazywaniu danych. Dlatego podjęto prace nad stworzeniem jednolitej regulacji prawnej we Wspólnocie Europejskiej. Efektem tych prac było przyjęcie przez Parlament Europejski i Radę w roku 1995 dyrektywy 95/46 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[21]. W dyrektywie 95/46 m.in.: uregulowano zasady przetwarzania danych osobowych, określono podstawy dopuszczalności przetwarzania danych, uprawnienia osób, których dane dotyczą, i obowiązki administratorów danych, nałożono na państwa członkowskie obowiązek powołania organu nadzorczego, wskazując zakres jego zadań, a także uregulowano kwestię transferu danych do państw trzecich[22]. Przepisy dyrektywy 95/46 odnosiły się również do podmiotów publicznych, w niektórych konstrukcjach prawnych można było zauważyć zamiar uwzględnienia przez prawodawcę specyfiki administracji publicznej (np. przy określaniu przesłanek dopuszczalności przetwarzania danych z uwagi na realizację zadań publicznych czy też uznaniu, że podmioty publiczne, które otrzymują dane osobowe w ramach prowadzonego postępowania, nie są uznawane za odbiorców tych danych).

[21] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, Dz.Urz. WE L 281, s. 31; Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, s. 355, ze zm.

[22] Szerzej na temat dyrektywy por. m.in. U. Dammann, S. Simitis, *EG-Datenschutzrichtlinie, Kommentar*, Baden-Baden 1997; E. Ehmann, M. Helfrich, *EG Datenschutzrichtlinie*, Köln 1999.

Dyrektywa 95/46 wymagała implementacji do prawa wewnętrznego państw członkowskich. Wszystkie państwa członkowskie dokonały wdrożenia wskazanej dyrektywy, przyjmując krajowe regulacje prawne dotyczące ochrony danych. Polska, ubiegając się o członkostwo w Unii Europejskiej, była także zobowiązana dostosować swoje prawodawstwo do wymogów określonych w dyrektywie 95/46. Warunek ten został spełniony wskutek uchwalenia w naszym kraju ustawy z 29.08.1997 r. o ochronie danych osobowych[23]. Ustawa ta miała zastosowanie zarówno do podmiotów prywatnych, jak i do podmiotów publicznych, w tym do administracji publicznej, w przypadku przetwarzania danych osobowych w sposób zautomatyzowany (w systemach informatycznych), a w zbiorach danych (kartotekach, skorowidzach, księgach, wykazach) – także przy przetwarzaniu danych w sposób niezautomatyzowany (ręcznie, na nośnikach papierowych). Na mocy przepisów ustawy o ochronie danych osobowych z 1997 r. nałożono na administratorów danych (również w administracji publicznej) wiele obowiązków[24], m.in.: obowiązek oparcia przetwarzania danych na odpowiedniej podstawie prawnej; obowiązki informacyjne, korekcyjne i szczególne; obowiązek dołożenia szczególnej staranności przy przetwarzaniu danych (przestrzegania zasad przetwarzania i ochrony danych); obowiązek zabezpieczenia przetwarzanych danych; obowiązek zgłoszenia zbioru danych do rejestracji, a przestrzeganie tych przepisów poddano nadzorowi wyspecjalizowanego organu – Generalnego Inspektora Ochrony Danych Osobowych[25]. W przepisach ustawy o ochronie danych osobowych z 1997 r. w niewielkim tylko stopniu uwzględniono specyfikę działalności administracji publicznej. Przepisy dotyczące przetwarzania i ochrony danych osobowych zawarte były także w licznych szczegółowych regulacjach prawnych – ustawach i rozporządzeniach wykonawczych.

[23] Dz.U. Nr 133, poz. 883.

[24] Na ten temat por. m.in. M. Ganczar, *Obowiązki administracji publicznej w zakresie ochrony danych osobowych* [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009, s. 111–125.

[25] Szerzej na temat ustawy o ochronie danych osobowych z 1997 r. por. w: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015 i wskazaną tam literaturę.

Wprowadzanie regulacji prawnych dotyczących przetwarzania danych osobowych spotkało się z krytyką także w kręgach administracji publicznej, z uwagi na to, że wymogi w zakresie ochrony danych były postrzegane jako ograniczenie możliwości wykorzystania potencjału technologicznego, a nowe obowiązki były niekiedy uciążliwe. Bardzo często podawano w wątpliwość sens regulacji mającej służyć ochronie osób, których dane dotyczą, uznając tego rodzaju wymogi za nieuzasadnione i zbędne. Wydaje się, że stosunkowo często krytyka ta była powodowana niezrozumieniem istoty i celu prawnej regulacji ochrony danych osobowych, a także brakiem świadomości zagrożeń. Krytycy często próbowali dowodzić, że dane osobowe nie wymagają ochrony, a dodatkowe obowiązki w tym zakresie nie są konieczne, stanowią jedynie niepotrzebne obciążenie dla administracji. Typowym przykładem tego rodzaju argumentacji było stwierdzenie, że „jeżeli osoba postępuje zgodnie z prawem, to nie ma się czego bać i nie powinna obawiać się także ujawnienia informacji, które jej dotyczą". Jednakże w koncepcji prawnej ochrony danych osobowych dane nie stanowią głównego przedmiotu ochrony, ich ochrona nie jest celem samym w sobie, a jedynie środkiem, który umożliwia osiągnięcie zasadniczego celu – ochrony osób przed negatywnymi konsekwencjami bezprawnego przetwarzania ich danych. Informacje o osobie powinny być chronione nie dlatego, że świadczą o niej źle (np. wskazują na fakt popełnienia czynu zabronionego – w tym przypadku odpowiednie służby i organy są uprawnione do przetwarzania takich danych), ale dlatego, że ich przetwarzanie może stanowić bezprawną ingerencję w sferę prywatności i prowadzić do negatywnych konsekwencji dla osoby, której dane dotyczą. Niektóre zarzuty formułowane pod adresem ówczesnej regulacji były jednak zasadne i zasługiwały na rozważenie[26]. Niekiedy krytyka przepisów o ochronie danych osobowych wynikała także z dokonywania niewłaściwej ich wykładni, prowadzącej do nadmiernie restrykcyjnego podejścia do

[26] Na przykład podawano w wątpliwość zasadność obowiązku zgłaszania zbiorów danych prowadzonych przez organy administracji do rejestracji organowi nadzorczemu, gdyż większość tych zbiorów miała charakter powtarzalny, a organ nadzorczy mógł czerpać wiedzę o ich istnieniu z przepisów prawa nakładających na organy administracji obowiązek przetwarzania danych.

przetwarzania danych[27]. Powodem tego rodzaju problemów niejednokrotnie było niezbyt precyzyjne sformułowanie brzmienia przepisów, które pociągało za sobą wątpliwości interpretacyjne. Ponadto nowe obowiązki w zakresie dokumentacji przetwarzania danych (wymóg nadawania upoważnień, wdrożenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych) postrzegane były jako biurokratyczne obciążenia niemające realnego wpływu na skuteczność mechanizmów ochrony danych. Bez wątpienia jednak wdrożenie przepisów o ochronie danych osobowych przyczyniło się do wzrostu świadomości społeczeństwa co do zagrożeń związanych z ingerencją w sferę prywatności i potrzeby ochrony osób, przed negatywnymi konsekwencjami mogącymi wynikać z niezgodnego z prawem przetwarzania danych osobowych.

Implementacja dyrektywy 95/46 w państwach członkowskich Unii Europejskiej doprowadziła do dalszego ujednolicenia przepisów, jednak nadal istniały znaczne różnice między krajowymi regulacjami, co prowadziło do różnego rodzaju problemów[28]. Ponadto gwałtowny rozwój technologiczny sprawił, że konstrukcje prawne zawarte w dyrektywie 95/46 nie przystawały do współczesnych technologii przetwarzania danych. Okazało się również, że przepisy o ochronie danych osobowych oceniane były jako nieskuteczne, gdyż nie pozwalały na realizację podstawowego celu, jaki określił prawodawca: zapewnienie ochrony osób, których dane dotyczą[29]. Przepisy te były często lekceważone, a administratorzy nie

[27] Typowymi przykładami tego rodzaju problemów były przypadki odmowy udostępniania danych podmiotom uprawnionym do ich uzyskania bądź odwoływanie się do zgody na przetwarzanie danych w sytuacji, gdy dopuszczalność przetwarzania danych wynikała wprost z przepisów prawa.

[28] Przykładem mogą być m.in. zróżnicowane wymogi dotyczące zgody na przetwarzanie danych sensytywnych – w wielu krajach przepisy wymagały wyraźnej zgody, natomiast w Polsce wymagana była zgoda na piśmie, co uniemożliwiało w praktyce pozyskiwanie tego rodzaju zgody za pomocą środków komunikacji elektronicznej (w tym przez internet). Podmioty prywatne podejmowały różnorodne działania, aby obejść tego rodzaju ograniczenia, np. tworzono spółki w innych państwach członkowskich UE, aby móc legalnie zbierać dane sensytywne w sieci.

[29] Na temat skuteczności regulacji w literaturze z zakresu prawa administracyjnego pisał m.in. Z. Kmieciak w pracy: *Skuteczność regulacji administracyjnoprawnej*, Łódź 1994. Problematyka skuteczności regulacji ochrony danych osobowych była również

spełniali wielu obowiązków[30], nie obawiając się negatywnych konsekwencji naruszenia[31]. Dostrzegając wskazane powyżej problemy, podjęto wysiłki zmierzające do reformy unijnych ram prawnych ochrony danych[32]. Zasadniczymi celami wyznaczonymi przez prawodawcę unijnego w ramach reformy były: ujednolicenie przepisów o ochronie danych w Unii Europejskiej; poszerzenie uprawnień osób, których dane dotyczą; wzmocnienie pozycji oraz zwiększenie roli organów nadzorczych oraz wprowadzenie administracyjnych kar pieniężnych za naruszenie przepisów o ochronie danych. Realizacja wskazanych powyżej założeń reformy miała przyczynić się do poprawy efektywności regulacji i umożliwienia bardziej skutecznego osiągnięcia głównych celów, jakim służyć mają przepisy o ochronie danych – ochrony osób fizycznych w związku z przetwarzaniem ich danych przy jednoczesnym zagwarantowaniu swobodnego przepływu danych w UE[33]. Efektem kilkuletnich prac było przygotowanie dwóch aktów normatywnych: ogólnego rozporządzenia o ochronie danych osobowych oraz tzw. dyrektywy policyjnej. Nowe przepisy weszły w życie w roku 2016, a zaczęły być stosowane po upływie dwuletniego okresu przejściowego – od 25.05.2018 r.

---

przedmiotem szczegółowych analiz, por. *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009.

[30] Najbardziej wyrazistym tego przykładem było powszechne lekceważenie wymogów prawnych dotyczących informowania o przetwarzaniu danych: wielu administratorów, w tym także ze sfery publicznej, nie dopełniało ciążącego na nich obowiązku informacyjnego, pomimo że zgodnie z art. 54 u.o.d.o.1997 niespełnienie tego obowiązku było uznawane za przestępstwo.

[31] Taki stan rzeczy wynikał po części z przekonania o niewielkiej (bądź nawet znikomej) szkodliwości społecznej naruszeń w zakresie ochrony danych, co było przyczyną rzadkiego podejmowania przez organy ścigania działań zmierzających do pociągnięcia sprawców do odpowiedzialności karnej. Z perspektywy czasu wydaje się, że przyjęcie przez prawodawcę reżimu odpowiedzialności za przestępstwa w przypadku niewielkich nawet naruszeń przepisów o ochronie danych osobowych, przy braku możliwości pociągnięcia sprawcy do odpowiedzialności „łagodniejszej" (np. za wykroczenia) nie było rozwiązaniem właściwym.

[32] Na temat reformy por. m.in. W.R. Wiewiórowski, *Nowe ramy ochrony danych osobowych w Unii Europejskiej* [w:] *Aktualne problemy prawnej ochrony danych osobowych 2012*, red. G. Sibiga, dodatek specjalny do MoP 2012/7, s. 2–9.

[33] Na temat celów prawnej regulacji ochrony danych por. A. Grzelak, *Główne cele ogólnego rozporządzenia o ochronie danych* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017, s. 11–23.

3. Specyfika przetwarzania i ochrony danych osobowych w administracji publicznej

Przetwarzanie danych osobowych w administracji publicznej wykazuje cechy specyficzne, które odróżniają te procesy od przetwarzania danych w sektorze prywatnym, co pociąga za sobą istotne konsekwencje w zakresie obowiązków związanych z ochroną danych osobowych. Można wskazać kilka zasadniczych elementów składających się na tę specyfikę.

Po pierwsze – administracja publiczna przetwarza dane osobowe w celu realizacji zadań publicznych, w odróżnieniu od podmiotów prywatnych, które realizują swoje własne, prywatne cele (np. cele komercyjne). Działania zmierzające do realizacji zadań publicznych podejmowane są w imieniu państwa, przy ich realizacji organy administracji dysponują władztwem administracyjnym, a więc mają możliwość jednostronnego kształtowania sytuacji prawnej (praw i obowiązków) podmiotów administrowanych (w tym osób fizycznych, których interesów dotyczą działania administracji). Z wymogu realizacji zadań publicznych wynika konieczność przetwarzania danych osobowych przez organy administracji. Działania organów administracji publicznej w zakresie przetwarzania danych osobowych są z reguły podejmowane w sferze imperium – są to działania władcze charakteryzujące się tym, że organy administracji mogą żądać od osób fizycznych podania danych i mogą przetwarzać dane osobowe bez zgody (niekiedy nawet wbrew woli) tych osób, a prawidłowe wykonywanie działań w tym zakresie zabezpieczone jest środkami przymusu i sankcjami. Działania administracji publicznej nie ograniczają się jednak wyłącznie do działań władczych i obejmują także formy niewładcze, jednak nie stanowią one dominującej aktywności administracji i mają niekiedy charakter uzupełniający względem działań władczych (np. działania informacyjne czy promocyjne). Warto wspomnieć także o tym, że administracja publiczna podejmuje również działania niewładcze w sferze *dominium* – np. w obszarze stosunków własnościowych, i wówczas procesy przetwarzania danych osobowych w administracji powinny być realizowane podobnie, jak w sektorze prywatnym.

Drugą charakterystyczną cechą przetwarzania danych osobowych przez administrację publiczną jest wykonywanie tych działań na podstawie i w granicach wyznaczonych przepisami prawa – wynikające z zasady legalizmu działań administracji publicznej. Organy administracji publicznej powinny przetwarzać dane osobowe nie tylko zgodnie z przepisami, ale także na ich podstawie i w zakresie w przepisach określonym. Istnieje wiele przepisów stanowiących podstawę przetwarzania danych osobowych przez organy administracji i określających cel, zakres, a niekiedy również sposób przetwarzania danych. Jednakże nadal istnieją obszary, w których realizacja zadań publicznych wymaga przetwarzania danych osobowych, a przepisy nie regulują wprost tej problematyki i nie zawierają wyraźnej podstawy prawnej, na którą mogłyby powoływać się organy administracji. Dlatego też konieczne jest zapewnienie możliwości przetwarzania danych osobowych w przypadku braku wyraźnego przepisu ze wskazaniem, że przetwarzanie danych jest dopuszczalne, jeśli jest niezbędne dla realizacji zadań publicznych. Przepisy prawa mogą stanowić nie tylko podstawę, na której opierać się będzie przetwarzanie danych, ale także barierę ograniczającą zakres tego przetwarzania, tak aby umożliwić realizację podstawowego celu regulacji ochrony danych osobowych – ochronę osób, których dane dotyczą, przed negatywnymi konsekwencjami wynikającymi z naruszającego porządek prawny przetwarzania danych. Z zasady legalizmu działań administracji wynika, że inne podstawy dopuszczalności przetwarzania danych (np. zgoda osoby, której dane dotyczą) mogą być wykorzystywane w administracji publicznej w ograniczonym zakresie, co do zasady jako przesłanki dodatkowe, uzupełniające. W odróżnieniu od podmiotów prywatnych, dla których podstawową zasadą działania jest wolność (m.in. swoboda działalności gospodarczej) i które mogą samodzielnie decydować o podejmowaniu działań, z którymi wiąże się przetwarzanie danych (pod warunkiem spełnienia wymogów określonych przepisami prawa), organy administracji publicznej ograniczone są w tym zakresie przepisami i mogą podejmować jedynie takie działania, które zostały w przepisach przewidziane.

Trzecią charakterystyczną cechą przetwarzania danych osobowych w administracji publicznej jest korzystanie przez organy administracji z rozległych zasobów informacyjnych administracji. Przy realizacji zadań publicznych wykorzystywane są dane, które pochodzą z różno-